UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/593,588	09/21/2006	Parminder Singh Mudhar	36-2021	1503

23117 7590 09/15/2009

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
WANG-HURST, KATHY W	

ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
09/15/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/593,588
Filing Date: September 21, 2006
Appellant(s): MUDHAR, PARMINDER SINGH

Chris Comuntzis
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 6/10/2009 appealing from the Office action mailed 12/10/2008.

(1) Real Party in Interest

A statement identifying by name the real partying interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6571221	**Stewart et al.**	**5-2003**
2003/0039234	**Sharma et al.**	**2-2003**

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart, herein referred as Stewart in view of Sharma et al. (US 2003/0039234), herein referred as Sharma, cited in applicant's IDS.

Regarding claim 1, Stewart discloses a method of authorizing data transfer to or from a mobile node temporarily connected to an attachment point of a network (see Abstract and col. 14 lines 15-35), the method including the steps of:

(a) receiving a digital certificate (see Fig. 4 item 216 receiving certificate), which certificate includes a message body and a digital signature for verifying the content of the message body (Abstract and col. 1 lines 40-67), the message body having geographical information therein (Abstract and col. 3 lines 33-44), which geographical information is derived from a physical location (col. 3 lines 33-44);

(b) performing a comparison between the geographical information of the certificate and

other information (col. 14 lines 29-33 comparing; col. 13 lines 33-44 using geographical information for authentication and security); and,

(c) making an authorization decision for data transfer to or from the mobile node in dependence on the result of the comparison (col. 15 lines 45-46 and Fig. 4 item 224, 226 and 236).

Stewart fails to disclose the digital certificate is from the forwarding node. Sharma teaches a forwarding node in an IP network ([0012] home agent intercepts packets and forward them to MN, therefore home agent is acting as a forwarding node) and an authentication process between the forwarding node and mobile node ([0013]-[0015] MN and home agent conduct internet security check).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Stewart's digital certificate retrieval system by Sharma's authentication system in order to extend the security function to an IP network when mobile unit roams to other networks and to allow forwarding node and mobile node to verify the data was not modified in transit, thus providing an improved security verification process ([0015]).

Regarding claim 2, Stewart discloses a method as claimed in claim 1, wherein the digital certificate is suitable for use in a public key encryption system (col. 1 lines 41-42).

Regarding claim 3, Stewart discloses a method as claimed in claim 2, wherein the certificate is having a public key and a private key associated therewith, and wherein the signature is a function, at least in part, of the private key of the certificate

node (col. 1 lines 41-55). Stewart fails to disclose that the certificate is generated at a certificating node. Sharma teaches an authentication mechanism generating keys from the mobile node and send the keys to a packet gateway node ([0008]). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Stewart's digital certificate retrieval system by Sharma's authentication system in order to further improve the security of the network through mutual authentication ([0008]) instead of one-way authentication.

Regarding claim 4, Stewart discloses a method as claimed in claim 2, including the step of verifying the authenticity of the digital certificate (col. 1 lines 41-42). Stewart fails to disclose the step of verifying the authenticity by performing a computation on at least part of certificate, the computation involving the public key associated with the certificate node. Sharma teaches the step of authentication involving mathematical algorithms and keys to that authentication algorithm ([0014] and [0016]). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate the authentication step taught by Sharma into the verifying step disclosed by Stewart in order to further improve the security of the network communication through a logically implemented authentication protocol ([0015]).

Regarding claim 5, Stewart discloses a method as claimed in claim 1, wherein the mobile node has a certificate associated therewith, which certificate includes geographical information, the method including the further step of receiving the

certificate from the mobile node, and using the geographical information from the certificate of the mobile node to make the authorisation decision (col. 2 lines 53-56).

Regarding claim 6, Stewart discloses a method as claimed in any of the preceding claims, wherein a registration procedure is performed to allow data transfer between the forwarding node and the mobile node, and wherein the registration procedure includes the steps of: receiving, at the forwarding node, a certificate with geographical information therein (Fig. 4 item 216); and, comparing the received geographical information with a further item of geographical information (Fig. 4 items 202, 204, 206, 208, and 216).

Regarding claim 7, Stewart discloses a method as claimed in claim 1, wherein the geographical information in the certificate associated with the forwarding node is derived from the physical location of the forwarding node (col. 2 lines 54-56).

Regarding claim 8, Stewart discloses a method as claimed in claim 1, wherein there is a mobile node (Abstract), but fails to disclose that the mobile node has a temporary address and a permanent address associated therewith. Sharma teaches a method and system for secure network roaming in which there is a temporary address ([0012]) and that permanent address ([0011]) such that the mobile device can retrieve messages through a temporary care-of address when it is away from the permanent address ([0012]). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate the temporary and permanent address in order to provide a better way to accommodate device mobility within the network ([0011]).

Regarding claim 9, Stewart discloses a method as claimed in claim 8, wherein the temporary address of the mobile node is indicative of the topological position of the current point of attachment of the mobile node (col. 10 lines 19-29 geographic information pinpointing the location of each access point).

Regarding claim 10, Stewart discloses a method as claimed in claim 8, but fails to disclose the steps. Sharma teaches the steps of:

(i) intercepting packets addressed to the permanent address of the mobile node ([0012]); and,

(ii) forwarding the intercepted packets towards the temporary address of mobile node ([0012]), at least one of steps (i) and (ii) being authorized in dependence on the result of a comparison involving geographic information within a certificate ([0007]).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate the packet forwarding steps taught by Sharma into the communication method disclosed by Stewart in order to provide a better way to accommodate device mobility within the network ([0011]).

Regarding claim 11, Stewart discloses a method as claimed in claim 1, wherein the forwarding node is a fixed node (col. 2 lines 43-56 Access points are located at airports, mass-transit stations therefore fixed nodes).

Regarding claim 12, Stewart discloses a method as claimed in claim 1, including an authentication step (col. 1 lines 18-19).

Claims 13-16 are rejected under 35 U.S.C. 102(a) as being anticipated by Stewart et al. (US 6571221).

Regarding claim 13, Stewart discloses a network node for authorizing the transfer of data to a mobile node temporarily connected to a forwarding node, wherein the network node is configured, in response to receiving a digital certificate from the forwarding node, to read at least part of the digital certificate, the digital certificate including geographical information derived from a physical location, and wherein the network node is further configured to: perform a comparison between the geographical information of the certificate and a further item of geographical information (Abstract); and, in dependence on the result of the comparison, make an authorization decision (Fig. 4 items 224, 226 and 236).

Regarding claim 14, Stewart discloses a method of authorizing data transfer to or from a mobile node using a digital certificate, wherein the digital certificate includes a message body, a digital signature for verifying the content of the message body, the message body having geographical information derived from a physical location, the method including the steps of: receiving the digital certificate from the mobile node (Fig. 4 item 216 receiving certificate); performing a comparison between the geographical information of the certificate and a further item of geographical information (col. 11 lines 1-11); and, making an authorization decision in dependence on the result of the comparison (Fig. 4 items 224, 226 and 236).

Regarding claim 15, Stewart discloses a method as claimed in claim 14, wherein the mobile node is configured to form a temporary attachment to an attachment point of a main network, and wherein the digital certificate is received at a network node in the

main network (col. 2 lines 43-56 mobile user is temporarily access network through an access point; and Fig. 4 items 216).

Regarding claim 16, Stewart discloses a method as Claimed in claim 15, wherein the attachment point has a forwarding node associated therewith for forwarding messages to and/or from the mobile node, and wherein the forwarding node has a digital certificate associated therewith, which certificate include geographical information derived from the physical location of the forwarding node, the method including the steps of: at the network node, receiving the digital certificate from the forwarding node (Fig. 4 item 216 receiving certificate; col. 11 lines 1-11); and,
making an authorization decision in dependence on the geographical information of the certificate from the forwarding node (Fig. 4 items 224, 226 and 236).

(10) Response to Argument

TECHNOLOGY BACKROUND

In a wireless communication network, a mobile user may access network services through an access point/base station. A mobile terminal accesses the network via a wirless channel, where the base station/access point receives the data and forwards the data to the system infrastructure, i.e., other devices such as servers, switches, exchanges or Websites, where the information finally reaches an end destination. Thus each device in turn acts as a forwarding device where information is forwarded from the mobile to an end point and from the end point to the mobile. Thus, the access point/base station can receive messages and forward messages to other

access points/base stations or servers or devices, and forward information from those devices back to the mobile. Before any forwarding of data in a wireless system both the mobile unit and the system must be authenticated so that data can not be intercepted and used for fraudulent purposes. Authentication typically is done by checking data that was stored when a user subscribes to service, such as, user or server name, serial numbers, passwords, addresses, etc. The number and types of data used for the authentication are variable depending on the level of security desired. When several pieces of this data are incorporated in one digital data object it is called a digital certificate. Depending on the level of security desired, the digital certificate may include many types of data. IN the forwarding process, *discussed above,* a digital certificate is used to authorize message transfers. Any forwarding node may ask for the digital certificate in order to make authorization decisions. The digital certificate stores user related information such as geographical information of the user and demographic information of the user. Once the information stored on the digital certificate is verified, the messages will be authorized to transfer.

SUMMARY OF APPELLANT'S ARGUMENT AND EXAMINER'S RESPONSE TO ARGUMENT

Appellant argues with respect to claims 1-16 that a digital certificate disclosed in Stewart does not contain geographical information.

Examiner respectfully disagrees. Stewart discloses a digital certificate that is used to access the network. Stewart discloses (abstract) that the digital certificate may include other information stored in it or within extensions of it, including geographic

location of the user. In further passages, Stewart also discloses the digital certificate stores user related information including geographic location of the user and demographic information of the user.

Therefore the examiner contends that Stewart indeed teaches a digital certificate that includes geographic information and the digital certificate is used to authorize data transfer.

DETAILS OF APPELLANT'S ARGUMENT AND EXAMINER'S RESPONSE

Brief pages 10-13: Appellant Argues Claims 1-12 are not obvious under USC 103(a) in view of Stewart and Sharma.

Brief Page 10, Appellant argues that the portions of Stewart relied upon, do not actually state geographic information is contained in the certificate:

Appellant argues with respect to claims 1-12 that Stewart does not disclose a digital certificate that contains the geographical information. The examiner respectfully disagrees. Stewart discloses a digital certificate may be stored on the mobile user's PCD in order to allow access to the network, and information stored on the digital certificate includes sponsorship information, the geographic location of the user, demographic information of the user, and charging information of the user (see Abstract and col. 3 lines 33-43). Therefore it is evident that Stewart discloses a digital certificate that contains geographical information of the user.

Brief Page 11, Appellant agues that the geographic information in Stewart is outside the certificate and that Stewarts Certificate is Unchangeable so that Location information cannot be included.

Appellant argues that the geographical information is outside the digital certificate (see Brief page 11) and the user is mobile user whose geographical location changes and therefore the geographical information cannot be in the certificate (see Brief page 11) . The examiner respectfully disagrees. Stewart discloses information in the digital certificate such as sponsorship information is used to provide incentives to the users who belong to certain sponsorship organizations, and geographical information to provide incentives for users to access the network from certain locations (col. 4 lines 18-36). Therefore it is evident that the geographical information is indeed contained in the digital certificate.

Brief Page 12, Appellant Argues that the geographic information is provided by the access points.

Appellant argues that the access points provide the geographical information and therefore the geographical information cannot be in a digital certificate (see Brief page 12). The examiner respectfully disagrees. Stewart discloses the geographical information of the mobile unit may be provided to the network through the access point. Just because the geographical information is transmitted to the network through access point does not mean the geographical information is not on the digital certificate (col. 3 lines 39-43). In addition, Stewart discusses providing incentives to use certain access locations based on the geographical information stored in the digital certificate. In other words, if the geographical information of the user and geographical information of the access points have to be transmitted and matched in order to obtain benefits of the

incentive (col. 3 lines 39-43 and col. 4 lines 18-36). Therefore it is clear that Stewart discloses a digital certificate that contains geographical information.

Brief Page 12-13, the Appellant argues necessity of the secondary reference, Sharma.

Concerning the appellant's arguments regarding the secondary reference Sharma (see Brief pages 12-13), Stewart discloses wired and wireless access points which may be forwarding nodes but Stewart does not explicitly disclose a forwarding node. Therefore Sharma was brought in to explicitly teach a forwarding node.

Therefore the examiner contends that claims 1-12 are obvious in view of Stewart and Sharma.

Brief pages 13: Appellant Argues Claims 13-16 are not anticipated under USC 102 in view of Stewart.

Regarding appellant's arguments on claims 13-16 (see Brief page 13), for the same reason given above with respect to the arguments of claims 1-12, Stewart discloses a digital certificate that contains geographical information of the user in claims 13-16. Therefore Stewart anticipates claims 13-16.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/KATHY WANG-HURST/

Examiner, Art Unit 2617

Conferees:

/NICK CORSARO/

Supervisory Patent Examiner, Art Unit 2617

/George Eng/

Supervisory Patent Examiner, Art Unit 2617